Кібербезпека
та захист критичної інфраструктури

УДК 004.056.5:004.021

КОМПАРАТИВНИЙ АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ МОДЕЛЮВАННЯ В КІБЕРБЕЗПЕЦІ

В.С. Кравчук[1], Т.В. Алтухова[1], Я.Ю. Дорогий[1, 2, 3]
[1] *Department of Applied Mathematics and Informatics, Donetsk National Technical University, Drohobych, Ukraine*
[2] *Department of Information Systems and Technologies, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine*
[3] *Department of Intelligent Software Systems, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine*

E-mail: yaroslav.dorohyi@donntu.edu.ua

АНОТАЦІЯ

Сучасний ландшафт кібербезпеки характеризується високою складністю та динамічністю, що зумовлює потребу в передових методах моделювання для аналізу загроз, прогнозування ризиків та оцінки ефективності захисних заходів. У цій статті представлено детальний компаративний аналіз традиційних і сучасних підходів до моделювання в кібербезпеці, включно з математичним, логічним та ієрархічним моделюванням, симуляціэю атак і Breach and Attack Simulation (BAS), агентно-орієнтованим моделюванням, цифровими двійниками, а також методи, що базуються на машинному навчанні, глибокому навчанні, теорії ігор, графових структурах і великих мовних моделях (LLM). Кожен метод розглянуто з погляду принципів роботи, ключових переваг, недоліків і практичного застосування. Особливу увагу приділено синергії та взаємодоповнюваності цих підходів, що є критично важливим для створення комплексних, адаптивних систем кібербезпеки. Традиційні методи, як-от математичне моделювання, забезпечують формальну основу для аналізу, але можуть спрощувати реальні сценарії. Сучасні підходи, зокрема машинне навчання та цифрові двійники, дають змогу обробляти великі обсяги даних і моделювати складні динамічні взаємодії, хоча потребують значних обчислювальних ресурсів і точних даних. Теорія ігор і графові моделі пропонують стратегічний і контекстуальний аналіз, тоді як великі мовні моделі відкривають нові можливості для автоматизації аналізу загроз, попри їх обмеження в надійності. Інтеграція цих методів створює основу для гібридних рішень, які компенсують недоліки окремих підходів, підвищуючи загальну ефективність захисту. Стаття також висвітлює виклики, пов’язані з обчислювальною складністю, невизначеністю й етичними аспектами, і окреслює майбутні напрями розвитку, зокрема вдосконалення пояснюваного ШІ, стійкість до змагальних атак і реалізм симуляцій.

Ключові слова: *кібербезпека, моделювання, машинне навчання, цифрові двійники, графові моделі, симуляція атак.*

Вступ

На сьогодні ландшафт кібербезпеки характеризується безпрецедентною складністю та динамічністю, що зумовлено стрімким розвитком технологій, глобалізацією цифрових систем і швидким зростанням кількості та різноманітності кіберзагроз [1–2]. Кібератаки вирізняються частотою, витонченістю та скоординованістю, включно з розширеними стійкими загрозами (APT), фішингом, атаками з використанням шкідливого програмного забезпечення, а також змагальними маніпуляціями, спрямованими на обхід систем захисту, зокрема тими, що базуються на штучному інтелекті [3–4]. Ця ескалація загроз перевищує можливості традиційних методів виявлення та запобігання, як-от сигнатурний аналіз чи статичні правила, які не здатні ефективно справлятися з динамічною природою атак [5].

Такий стан справ створює нагальну потребу в інноваційних підходах до моделювання, які можуть обробляти величезні обсяги даних, виявляти приховані закономірності, прогнозувати поведінку зловмисників і оцінювати ефективність захисних механізмів у реальному часі [5]. Традиційні методи аналізу загроз, а саме математичне чи логічне моделювання,

Copyright © 2025, ОТА.

стикаються зі значними труднощами через складність і мінливість кібератак, що спонукає до розробки адаптивних і інтелектуальних моделей, як-от глибоке навчання, агентно-орієнтоване моделювання, цифрові двійники та графові структури [6].

Моделювання відіграє ключову роль у кібербезпеці, надаючи можливість дослідникам, інженерам і фахівцям із безпеки вивчати поведінку мереж і систем у контрольованих віртуальних середовищах. Це дає змогу оцінювати їхню продуктивність, оптимізувати конфігурації, виявляти потенційні вразливості та тестувати стратегії захисту ще до розгортання в реальних умовах [7]. Крім того, моделювання сприяє проактивному підходу до кіберзахисту, завдяки чому можна передбачати нові вектори атак і розробляти стратегії реагування на них. У контексті зростаючої складності кіберзагроз і появи нових технологій, як-от інтернет речей (IoT), хмарні обчислення та квантові технології, потреба в комплексних, гібридних моделях, які поєднують переваги різних методів, стає критично важливою. Таким чином, розробка й інтеграція передових методів моделювання є ключовими для забезпечення стійкості кіберсистем до нових і непередбачуваних загроз, тож тема дослідження є актуальною.

Постановка проблеми дослідження

Ключовою проблемою є обмежена здатність традиційних методів моделювання, як-от математичне чи логічне моделювання, враховувати динамічну природу кіберзагроз, поведінку користувачів і складні взаємодії в гетерогенних мережевих середовищах. Водночас сучасні підходи, а саме машинне навчання, агентно-орієнтоване моделювання чи цифрові двійники, хоча й пропонують нові можливості, стикаються з викликами, пов'язаними з високими обчислювальними вимогами, необхідністю якісних даних, вразливістю до змагальних атак і недостатньою прозорістю рішень. Відсутність універсального методу, який би поєднував переваги різних підходів, ускладнює створення комплексних і адаптивних систем кібербезпеки.

Таким чином, виникає потреба в систематичному аналізі та порівнянні традиційних і сучасних методів моделювання, оцінці їхньої ефективності, виявленні можливостей синергії та визначенні перспективних напрямів розвитку для підвищення стійкості кіберзахисту в умовах зростаючої складності загроз.

З огляду на вищенаведене метою цього дослідження є надання детального компаративного аналізу методів і технологій моделювання, застосовних у кібербезпеці, з акцентом на їхню ефективність, сфери використання та потенціал інтеграції.

Для досягнення цієї мети систематизовано традиційні та сучасні підходи, проаналізовано їхні особливості, проведено порівняльну оцінку та визначено ключові виклики й перспективи розвитку.

Матеріали та методи дослідження

Дослідження зосереджено на порівнянні методів моделювання в кібербезпеці, використовуючи наукові публікації, технічні звіти й огляди з авторитетних джерел, а саме Nature, Springer, MDPI, arXiv, а також матеріали організацій, зокрема XM Cyber і Picus Security, до 2025 року. Аналіз охопив літературу про математичне, логічне, симуляційне, агентно-орієнтоване моделювання, цифрові двійники, машинне навчання, теорію ігор, графові моделі та великі мовні моделі. Кейси застосування, як-от Purdue-модель, фреймворк AMM, платформи BAS (SCYTHE, AttackIQ) і графові інструменти (Neo4j, Maltego), стали основою для оцінки практичної реалізації методів.

Для аналізу застосовано фундаментальні та прикладні методи. Аналіз і синтез допомогли систематизувати характеристики методів, порівняльний аналіз зіставив традиційні та новітні підходи за ефективністю, масштабованістю й адаптивністю, а системний підхід розглядав методи як взаємопов'язані елементи кібербезпеки. Огляд літератури та класифікація методів дали змогу зібрати дані про принципи роботи і приклади застосування, тоді як порівняльна оцінка, зокрема BAS проти тестування на проникнення, виявила їхні сильні та слабкі сторони. Аналіз кейсів (наприклад, використання CrowdStrike для машинного навчання чи GALLIUM APT для агентного моделювання) доповнив дослідження.

Методологічно дослідження базувалося на об'єктивності й науковій достовірності, використовуючи програмні інструменти для систематизації літератури (Mendeley, Zotero) та обробки текстів. Поєднання фундаментальних методів, зокрема абстрагування для виділення ключових аспектів, із прикладними, як-от аналіз кейсів, забезпечило цілісне розуміння методів моделювання. Особливу увагу приділено синергії підходів, що є основою для створення адаптивних систем кіберзахисту.

Аналіз методів і технологій моделювання

Моделювання в кібербезпеці передбачає створення формальних або віртуальних представлень комп'ютерних і кіберфізичних систем для аналізу загроз, прогнозування ризиків і оцінки захисних заходів [8]. Традиційні методи, як-от математичне, ієрархічне та логічне моделювання, базуються на формалізації безпекових властивостей через математичні структури [9], тоді як сучасні підходи використовують обчислювальні експерименти та інтелектуальну обробку даних для відтворення поведінки складних систем.

Математичне моделювання застосовує рівняння, ймовірнісні моделі, теорію графів, теорію ігор

і диференціальні рівняння для опису систем і загроз [10]. Наприклад, у дослідженні Суфі та Альсуламі запропоновано фреймворк, що поєднує χ^2-тести, баєсівський аналіз і кластерний аналіз для виявлення статистичних закономірностей у кібератаках [4]. Ці моделі забезпечують відтворювані результати, дають змогу застосовувати аналітичні методи для обробки великих даних і є масштабованими, але їхня ефективність обмежується спрощенням реальних умов, що ігнорує поведінку користувачів чи динамічні змінні, а також складністю реалізації [11–12]. Математичні моделі використовуються для прогнозування вторгнень, аналізу стратегій «захисник – атакуючий» за допомогою теорії ігор і симуляції поширення шкідливого програмного забезпечення через диференціальні рівняння [13].

Переходячи до *ієрархічних моделей*, варто зазначити, що вони структурують системи на багаторівневі підсистеми з різними рівнями контролю, як, наприклад, Purdue-модель для промислових систем, що розділяє мережу на рівні від польових пристроїв до корпоративної інфраструктури [14]. Такий підхід спрощує розмежування доступу, сприяє впровадженню принципів «захисту в глибину» і забезпечує прозорість архітектури, але може не враховувати складну динаміку між рівнями, що ускладнює моделювання комплексних атак, а жорсткі межі можуть знижувати гнучкість системи [15–16]. Ієрархічні моделі, зокрема дерева атак, також дають можливість розбити складні загрози на підзадачі, що полегшує їхній аналіз [16].

Логічні моделі, або формальні методи, базуються на строгих математичних підходах, як-от процесна алгебра чи формальна логіка [9]. Наприклад, Пітер Райан застосував формалізм CSP для моделювання вимог безпеки [10]. Завдяки цим методами можна верифікувати безпекові властивості системи, виявляти суперечності та забезпечувати однозначні специфікації, що є особливо цінним для перевірки криптографічних протоколів через інструменти ProVerif або Tamarin, а також для формалізації властивостей безпеки за допомогою мови Event-B і платформи Rodin [9, 15]. Проте їхня складність обмежує використання у великих системах, а ігнорування людського фактора чи неформальних процедур знижує практичну цінність [9].

Сучасні методи моделювання, на відміну від традиційних, спираються на обчислювальні експерименти та інтелектуальну обробку даних [8]. Симуляційні моделі відтворюють поведінку системи у віртуальному середовищі, даючи можливість тестувати сценарії безпеки без ризику для реальних ресурсів [7]. Вони використовуються в кіберполігонах, мережевих емуляторах, як-от OMNeT++ і ns-3, а також у моделях епідеміології кібератак, наприклад CICEД для комп’ютерних вірусів [18]. Симуляція атак імітує реальні загрози для оцінки захисних механізмів, сприяючи тренуванню фахівців і оцінці політик безпеки [17]. Точність таких симуляцій залежить від якості моделі, але вони можуть не враховувати всіх реальних факторів, що іноді створює хибне відчуття безпеки [7]. Наприклад, платформа Hoxhunt пропонує симуляції фішингу для підвищення обізнаності працівників [19]. Платформи BAS забезпечують безперервну автоматизовану перевірку стану безпеки, імітуючи тактики MITRE ATT&CK, виявляючи слабкі місця та надаючи рекомендації [20]. Для порівняння: управління вразливостями (VM) ідентифікує та пріоритизує відомі вразливості за допомогою автоматизованих сканерів, тестування на проникнення передбачає ручний і інструментальний аналіз для виявлення експлуатованих вразливостей, а BAS пропонує безперервну валідацію в реальному часі [21–23]. VM забезпечує широке покриття, але може давати хибні спрацювання, Pentesting пропонує глибокий аналіз, але є періодичним і часозатратним, тоді як BAS вирізняється масштабованістю й економічною ефективністю, хоча залежить від актуальності бібліотеки загроз. Провідними BAS-платформами є SCYTHE, Google Mandiant, Cymulate, AttackIQ, SafeBreach, Picus Security, FourCore ATTACK, Pentera, XM Cyber і SnapAttack [23].

Агентно-орієнтоване моделювання (ABM) представляє систему як сукупність автономних агентів, що взаємодіють між собою та із середовищем [24, 44]. Цей підхід дає змогу моделювати боротьбу між атакуючими та захисниками, як у кейсі GALLIUM APT, де захисники, навчені за допомогою багатоагентного навчання з підкріпленням, підвищують ефективність [26]. ABM також ефективно аналізує поширення шкідливого програмного забезпечення, враховуючи локальну мережеву структуру та мобільність користувачів, як у фреймворку AMM [25, 27]. Моделі ABM забезпечують детальний аналіз взаємодій, дають змогу налаштувати правила з реальними параметрами та виявляти вразливі топології, але потребують значних обчислювальних ресурсів, тривалої верифікації та якісних даних для тестування [25].

Цифрові двійники створюють віртуальні копії реальних систем із синхронізацією даних у реальному часі, даючи можливість тестувати зміни без впливу на фізичну інфраструктуру [2]. Наприклад, Purdue University спільно з Boeing розробили цифровий двійник авіаційних систем для моделювання бортових мереж [2]. Ці моделі забезпечують детальну симуляцію, проактивний моніторинг аномалій і можливість тренувань, але їх розробка є ресурсомісткою, а відсутність стандартів і вразливість платформ ускладнюють масштабування [2, 28].

Моделі на основі штучного інтелекту, зокрема машинного (ML) і глибокого навчання (DL),

Copyright © 2025, ОТА.

використовують дані для прогнозування та виявлення загроз [3]. ML застосовується для аналізу мережевого трафіку, виявлення шахрайства та прогнозування атак, використовуючи такі моделі, як Support Vector Machines (SVM), Decision Trees, Random Forests, K-Nearest Neighbors (KNN) і Naive Bayes [29]. Наприклад, CrowdStrike аналізує дані кінцевих пристроїв, а Montimage виявляє атаки типу Cache Poisoning [30, 31]. ML-моделі вирізняються швидкістю, точністю й адаптивністю, але потребують перенавчання за зміни умов і вразливі до змагальних атак [12]. Пояснюваний ШІ (XAI) є важливим для підвищення прозорості рішень ML [12]. DL, як розширення ML, ефективно обробляє великі набори даних, автоматично вилучаючи ознаки, і застосовується для виявлення шкідливого програмного забезпечення на платформах Windows, Linux і Android через моделі MLP, RNN, LSTM, GRU, CNNs, ResNet, GANs і GNNs [32]. DL також використовується для виявлення вразливостей у коді через шість фаз: побудова набору даних, визначення гранулярності вразливостей, представлення коду, проєктування моделі, оцінка продуктивності та впровадження [33]. Однак DL-моделі стикаються з проблемами перенавчання, високими обчислювальними вимогами, низькою пояснюваністю та вразливістю до змагальних атак [32]. Для порівняння: Naive Bayes ефективний для великих даних і швидкого виявлення спаму, але має низьку точність у складних сценаріях; Decision Trees чіткі та зрозумілі, але обмежені в узагальненні; Random Forests стійкі до шуму, але залежать від даних; KNN ефективний для аномалій, але обмежений в обробці певних типів даних; SVM обробляє багатовимірні дані, але залежить від характеристик даних; DL-моделі (VGG, ResNet, Inception) виявляють складні патерни, але мають високі обчислювальні витрати; Extra Trees вирізняються точністю, але також залежать від даних [34]. Усі ці моделі потребують якісних даних, частого перенавчання та стійкості до змагальних атак.

Теорія ігор аналізує стратегічну взаємодію між зловмисниками та захисниками, застосовуючись для оптимізації систем виявлення вторгнень, аналізу APT, захисту з рухомою ціллю й обміну інформацією про загрози [35]. Цей підхід забезпечує математично обґрунтовані рішення, враховуючи реакції зловмисників на захисні політики, але обмежений припущеннями про повну інформацію та складністю врахування невизначеності.

Графові моделі, як-от графи знань, графи атак і графові нейронні мережі (GNNs), кодують взаємозв'язки між сутностями для аналізу загроз [8]. Графи знань представляють сутності як вузли, а відносини – як ребра, ефективно виявляючи аномалії та збагачуючи кіберрозвідку, але потребують фільтрації надлишкової інформації [36]. Графи атак візуалізують шляхи атаки, сприяючи пріоритизації ризиків, і підтримуються інструментами, а саме PuppyGraph, Neo4j, OWASP Amass, Maltego і Linkurious [8, 37]. GNNs моделюють складні залежності, підвищуючи ефективність систем виявлення вторгнень і аналізу вразливостей [38–39].

Великі мовні моделі (LLMs) вирізняються контекстуальним розумінням і генерацією людиноподібного тексту, застосовуючись для виявлення вразливостей, аналізу шкідливого програмного забезпечення, фішингу, вебфаззингу, збагачення кіберрозвідки, пошуку загроз і моделювання багатоагентних систем у симуляціях реагування на інциденти [40–42]. Проте їхня ненадійність, непослідовність і недостатнє калібрування обмежують використання в критичних сценаріях [43].

Обговорення та перспективи розвитку дослідження

Ефективність моделювання в кібербезпеці залежить від інтеграції різних методів, що дає змогу компенсувати їхні обмеження. Наприклад, поєднання графових нейронних мереж із глибоким навчанням підвищує точність виявлення атак, а великі мовні моделі збагачують графи знань для аналізу загроз. Симуляційні середовища, зокрема BAS, дають можливість тестувати стратегії, виведені за допомогою теорії ігор чи агентно-орієнтованого моделювання, у динамічних умовах. Формальні методи забезпечують верифікацію критичних компонентів, тоді як машинне навчання й симуляції виявляють непередбачені загрози. Штучний інтелект відіграє роль інтегруючого елемента, автоматизуючи аналіз і підвищуючи адаптивність моделей. Для вибору методів слід враховувати специфіку завдань: глибоке навчання і GNNs підходять для виявлення складних загроз, теорія ігор і ABM – для стратегічного планування, BAS і тестування на проникнення – для оцінки стійкості, формальні методи – для критичних систем, а LLMs – для автоматизації аналізу тексту. Майбутні дослідження слід зосередити на розвитку гібридних моделей, що інтегрують машинне навчання, агентно-орієнтоване моделювання та формальні методи, а також на вдосконаленні пояснюваного ШІ для підвищення прозорості рішень. Важливими напрямами є стійкість моделей до змагальних атак, моделювання невизначеності в теорії ігор і ABM, підвищення реалізму симуляцій через якісні набори даних, а також вирішення етичних питань, як-от упередженість моделей і конфіденційність даних.

Висновки

Дослідження компаративного аналізу методів моделювання в кібербезпеці показало, що ефективне протистояння складним і динамічним кіберзагрозам

потребує комплексного підходу, який поєднує традиційні та інноваційні методи. За результатами систематизації та порівняння підходів встановлено, що математичне та логічне моделювання забезпечують формальну основу для аналізу безпеки, але мають обмеження в умовах динамічних сценаріїв через спрощення реальних взаємодій. Симуляційні технології, зокрема BAS, виявилися ефективними для проактивної оцінки захисних механізмів, забезпечуючи безперервну валідацію та виявлення слабких місць. Агентно-орієнтоване моделювання та цифрові двійники продемонстрували здатність відтворювати складні взаємодії в гетерогенних системах, хоча їхнє впровадження ускладнене високими обчислювальними вимогами.

Методи штучного інтелекту, як-от машинне та глибоке навчання, показали високу точність у прогнозуванні та виявленні загроз, але їхня ефективність залежить від якості даних і вразлива до змагальних атак. Теорія ігор і графові моделі, включно з графами знань та графовими нейронними мережами, забезпечують стратегічний і контекстуальний аналіз, даючи змогу виявляти приховані шляхи атак і оптимізувати захисні стратегії. Великі мовні моделі відкривають перспективи для автоматизації кіберрозвідки, однак їхня ненадійність у реальних сценаріях потребує додаткового калібрування.

Основним результатом дослідження є підтвердження, що інтеграція різних методів моделювання дає змогу компенсувати їхні індивідуальні недоліки, створюючи гнучкі й адаптивні системи кібербезпеки. Зокрема, поєднання графових моделей із глибоким навчанням, симуляцій із теорією ігор та формальних методів із машинним навчанням забезпечує синергію, що підвищує загальну ефективність захисту. Дослідження також визначило ключові виклики, як-от потреба в пояснюваному ШІ, стійкості до маніпуляцій і реалізмі симуляцій, що окреслюють перспективні напрями подальшого розвитку цього дослідження.

Конфлікт інтересів

Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов'язаних даних.

ЛІТЕРАТУРА

[1] S. A. Sharaf, M.A.A. Al-qaness, M.A. Alghamdi, A.S. Alqahtani, A.M. Alshahrani, "Advanced mathematical modeling of mitigating security threats in smart grids through deep ensemble model," Sci. Rep., vol. 14, no. 23069, Oct. 2024. DOI: 10.1038/s41598-024-74733-6. URL: https://surl.lu/umzyfz. Дата звернення: 15.06.2025.

[2] M. Homaei, Ó. Mogollón-Gutiérrez, J. Carlos Sancho, M. Ávila & A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," Artif. Intell. Rev., vol. 57, no. 201, Jul. 2024. DOI: 10.1007/s10462-024-10805-3. URL: https://surl.li/asmirk. Дата звернення: 15.06.2025.

[3] I. Vourganas, A.L. Michala, "Applications of machine learning in cyber security: A review," J. Cybersecurity Privacy, vol. 4, no. 4, pp. 972–992, Dec. 2024. DOI: 10.3390/jcp4040045. URL: https://surl.li/vdlxkl. Дата звернення: 15.06.2025.

[4] F. Sufi and M. Alsulami, "Mathematical modeling and clustering framework for cyber threat analysis across industries," *Mathematics*, vol. 13, no. 4, p. 655, Feb. 2025. DOI: 10.3390/math13040655. URL: https://surl.li/fgrjnf. Дата звернення: 15.06.2025.

[5] Y. Miao, L. Pan, et al., "Machine learning based cyber attacks targeting on controlled information: A survey," arXiv:2102.07969, Feb. 2021 URL: https://surl.li/hmyhes. Дата звернення: 15.06.2025.

[6] J. Vitorino, I. Praça, E. Maia, L. Sousa, and S. Jardim, "A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection," arXiv:2111.13149, Nov. 2021. URL: https://surli.cc/vlcuxu. Дата звернення: 15.06.2025.

[7] H. Kavak, J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore, and S. Shetty, "Simulation for cybersecurity: State of the art and future directions," *J. Cybersecurity*, vol. 7, no. 1, p. tyab005, Mar. 2021. DOI: 10.1093/cybsec/tyab005. URL: https://surl.lu/crguxz. Дата звернення: 15.06.2025.

[8] XM Cyber, "Seeing what attackers see: How attack graphs help you stay ahead," Jan. 2025. URL: https://surli.cc/dfwcym. Дата звернення: 15.06.2025.

[9] S. Chong, J. Guttman, A. Datta, A. Myers, B. Pierce, P. Schaumont, T. Sherwood, N. Zeldovich, "Report on the NSF Workshop on Formal Methods for Security," arXiv:1608.00678, Aug. 2016. URL: https://surl.gd/sgrcyr. Дата звернення: 15.06.2025.

[10] P.Y.A. Ryan, "Mathematical Models of Computer Security," in Foundations of Security Analysis and Design (FOSAD 2000), vol. 2171, Lecture Notes in Computer Science, R. Focardi and R. Gorrieri, Eds. Berlin, Germany: Springer, 2001, pp. 1–62. DOI: 10.1007/3-540-45608-2_1. URL: https://surl.li/egqhjf. Дата звернення: 15.06.2025.

[11] F.S. Passino, N.M. Adams, E.A.K. Cohen, M. Evangelou, and N.A. Heard, "Statistical Cybersecurity: A Brief Discussion of Challenges, Data Structures, and Future Directions," Harvard Data Science Review, vol. 5, no. 1, Mar. 2023. DOI: 10.1162/99608f92.240383c7. URL: https://surli.cc/foscla. Дата звернення: 15.06.2025.

Copyright © 2025, ОТА.

[12] P. Mahadevappa, S.M. Muzammal, and R.K. Murugesan, "A Comparative Analysis of Machine Learning Algorithms for Intrusion Detection in Edge-Enabled IoT Networks," arXiv:2111.01383, Nov. 2021. URL: https://surl.li/zwaisx. Дата звернення: 15.06.2025.

[13] K. Mohamed, "Machine learning techniques to address cybersecurity," arXiv:2302.12415, Feb. 2023. URL: https://surl.lu/tdmavn. Дата звернення: 15.06.2025.

[14] D. Garton, "Purdue model framework for industrial control systems & cybersecurity segmentation," U.S. Dept. Energy/National Petroleum Council, Topic Paper 4–14, Jul. 2019. URL: https://surli.cc/fmkjby. Дата звернення: 15.06.2025.

[15] I. Sayar, N. Messe, S. Ebersold, and J.M. Bruel, "From What to How: A Taxonomy of Formalized Security Properties," arXiv:2505.14514, May 2025. URL: https://surl.lu/nwovtz. Дата звернення: 15.06.2025.

[16] Wikipedia, "Attack trees," Jan. 2025. URL: https://surl.li/dbzvmq. Дата звернення: 15.06.2025.

[17] Picus Security, "What is attack simulation," Jan. 2025. URL: https://surl.li/cifqpc. Дата звернення: 15.06.2025.

[18] Pynetlabs, "Top 10 network simulation tools," Jan. 2025. URL: https://surl.li/qesago. Дата звернення: 15.06.2025.

[19] Hoxhunt, "Cyber Security Simulation Training: How it Works + Best Practices," Jan. 2025. URL: https://surl.li/cbjkeq. Дата звернення: 15.06.2025.

[20] Picus Security, "Everything You Need to Know About BAS Tools," Jan. 2025. URL: https://surli.cc/exllfj. Дата звернення: 15.06.2025.

[21] Softprom, "Vulnerability management vs. penetration testing vs. breach and attack simulation," Jan. 2025. URL: https://surl.li/afkwyc. Дата звернення: 15.06.2025.

[22] CyberProof, "Penetration Testing vs Breach and Attack Simulator: Key Differences and Why It Matters," Jan. 2025. URL: https://surl.li/nxbard. Дата звернення: 15.06.2025.

[23] SCYTHE, "Top 10 breach and attack simulation (BAS) tools," Jan. 2025. URL: https://surli.cc/ujxueh. Дата звернення: 15.06.2025.

[24] A. Vestad and B. Yang, "A survey of agent-based modeling for cybersecurity," in *AHFE Open Access Proceedings*, vol. 127, pp. 83–93, Jul. 2024. URL: https://surl.lu/wcoxjx. Дата звернення: 15.06.2025.

[25] F.K. Batista, A.M. del Rey, and A. Queiruga-Dios, "A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks," Mathematics, vol. 8, no. 3, p. 410, Mar. 2020. DOI: 10.3390/math8030410. URL: https://surl.li/yvuqfp. Дата звернення: 15.06.2025.

[26] J. Soule, J. Jamont, M. Occello, P. Theron, and L. Traonouez, "Towards a multi-agent simulation of cyber-attackers and cyber-defenders battles," arXiv:2506.04849, Jun. 2025. URL: https://surl.li/jrkiup. Дата звернення: 15.06.2025.

[27] A. Bose, and K. Shin, "Agent-based modeling of malware dynamics in heterogeneous environments," *Security and Communication Networks*, vol. 6, no. 12, pp. 1–8, Dec. 2013. URL: https://surl.li/akjovc. Дата звернення: 15.06.2025.

[28] E.C. Balta, M. Pease, J. Moyne, K. Barton, and D.M. Tilbury, "Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems," IEEE Transactions on Automation Science and Engineering, vol. 21, no. 3, pp. 3245–3260, Jul. 2024. DOI: 10.1109/TASE.2023.3243147.

[29] K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, S. Chen, D. Liu, and J. Li, "Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity," Energies, vol. 13, no. 10, p. 2509, May 2020. DOI: 10.3390/en13102509.

[30] CrowdStrike, "CrowdStrike machine learning in cybersecurity," Jan. 2025. URL: https://surl.li/yfqmjm. Дата звернення: 15.06.2025.

[31] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Brdalo Rapa, A.V. Grammatopoulos, and F. Di Franco, "The Role of Machine Learning in Cybersecurity," Digital Threats: Research and Practice, vol. 4, no. 1, Art. no. 8, pp. 1–38, Mar. 2023. DOI: 10.1145/3545574. URL: https://surl.li/rpjhxe. Дата звернення: 15.06.2025.

[32] P. Maniriho, A.N. Mahmood, and M.J.M. Chowdhury, "Deep learning models for detecting malware attacks," arXiv:2209.03622, Jan. 2024 URL: https://surl.li/kvdwjl. Дата звернення: 15.06.2025.

[33] M.N. Uddin, Y. Zhang, and X. Hei, "Deep learning aided software vulnerability detection: A survey," arXiv:2503.04002, Mar. 2025. URL: https://surl.li/njcajz. Дата звернення: 15.06.2025.

[34] M. Hesham, M. Essam, M. Bahaa, A. Mohamed, M. Gomaa, M. Hany, and W. Elsersy, "Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection," arXiv:2407.06014, Jul. 2024. URL: https://surl.li/grzpge. Дата звернення: 15.06.2025.

[35] B. Collins, S. Xu, and P.N. Brown, "Game-Theoretic Cybersecurity: the Good, the Bad and the Ugly," arXiv:2401.13815, Jan. 2024. URL: https://surl.li/jkxpct. Дата звернення: 15.06.2025.

[36] L. Zhang, Q. Zhu, and Y. Xie, "Improving network threat detection by knowledge graph, large language model, and imbalanced learning," arXiv:2501.16393, May. 2025. URL: https://surli.cc/bqlnzd. Дата звернення: 15.06.2025.

[37] PuppyGraph, "Cyber Graph: Enhancing Cybersecurity with Graph Intelligence," Jan. 2025. URL: https://surl.li/yfugrw. Дата звернення: 15.06.2025.

[38] X. Zhang, "Graph neural networks in network security: From theoretical foundations to applications," in *Proc. Americas Conf. Inf. Syst. (AMCIS)*, Aug. 2025, pp. 1–10. URL: https://surli.cc/wpkgob. Дата звернення: 15.06.2025.

[39] V. Khurana and N. Kumar, "Graph Neural Networks for Cybersecurity Applications in Network Intrusion and

Vulnerability Analysis," in RADemics Research Institute, Chapter 8, Jan. 2025. URL: https://surl.li/tchiff. Дата звернення: 15.06.2025.

[40] Bolster.ai, "Large Language Models for Cybersecurity: The Role of LLMs in Threat Hunting," Apr. 2025. URL: https://surl.li/olyczz. Дата звернення: 15.06.2025.

[41] H. Xu, and et al., "Large language models for cyber security: A systematic literature review," arXiv:2405.04760, Jul 2024. URL: https://surl.li/coqqui. Дата звернення: 15.06.2025.

[42] Z. Liu, "Multi-Agent Collaboration in Incident Response with Large Language Models," arXiv:2412.00652, Dec. 2024. URL: https://surl.li/aghvvq. Дата звернення: 15.06.2025.

[43] E. Mezzi, F. Massacci, and K. Tuma, "Large language models are unreliable for cyber threat intelligence," arXiv:2503.23175, Mar. 2025. URL: https://surl.lu/xonjqn. Дата звернення: 15.06.2025.

[44] В. С. Кравчук, Н. О. Маслова та Я. Ю. Дорогий, "Автоматизований пошук XSS-вразливостей у веб-застосунках на основі мультиагентного підходу," Наукові праці ДонНТУ. Серія "Обчислювальна техніка та автоматизація", т. 3, № 4 (36), с. 13–26, 2025. DOI: 10.31474/2786-9024/v3i4(36).324435.

COMPARATIVE ANALYSIS OF MODELING METHODS AND TECHNOLOGIES IN CYBERSECURITY

Vladyslav Kravchuk, Tatiana Altukhova, Iaroslav Dorohyi

The cybersecurity landscape is characterized by high complexity and dynamism, necessitating advanced modeling methods for threat analysis, risk prediction, and evaluation of protective measures. This article presents a detailed comparative analysis of traditional and contemporary modeling approaches in cybersecurity, including mathematical, logical, and hierarchical modeling, attack simulations and Breach and Attack Simulation (BAS), agent-based modeling, digital twins, as well as methods based on machine learning, deep learning, game theory, graph structures, and large language models (LLMs). Each method is examined in terms of its operational principles, key advantages, limitations, and practical applications. Particular attention is given to the synergy and complementarity of these approaches, which are critical for developing comprehensive and adaptive cybersecurity systems. Traditional methods, such as mathematical modeling, provide a formal basis for analysis but may oversimplify real-world scenarios. Contemporary approaches, including machine learning and digital twins, enable the processing of large data volumes and modeling of complex dynamic interactions, though they require significant computational resources and accurate data. Game theory and graph models offer strategic and contextual analysis, while large language models open new possibilities for automating threat analysis, despite their reliability limitations. The integration of these methods forms the foundation for hybrid solutions that mitigate the shortcomings of individual approaches, enhancing overall protection efficacy. The article also highlights challenges related to computational complexity, uncertainty, and ethical considerations, and outlines future directions, such as improving explainable AI, resilience to adversarial attacks, and simulation realism.

Keywords: *cybersecurity, modeling, machine learning, digital twins, graph models, attack simulation.*

REFERENCES

[1] S.A. Sharaf, M.A.A. Al-qaness, M.A. Alghamdi, A.S. Alqahtani, A.M. Alshahrani, "Advanced mathematical modeling of mitigating security threats in smart grids through deep ensemble model," Sci. Rep., vol. 14, no. 23069, Oct. 2024. DOI: 10.1038/s41598-024-74733-6. [Online]. URL: https://surl.lu/umzyfz. Accessed: 15 Jun, 2025.

[2] M. Homaei, Ó. Mogollón-Gutiérrez, J. Carlos Sancho, M. Ávila & A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," Artif. Intell. Rev., vol. 57, no. 201, Jul. 2024. DOI: 10.1007/s10462-024-10805-3. [Online]. URL: https://surl.li/asmirk. Accessed: 15 Jun, 2025.

[3] I. Vourganas, A.L. Michala, "Applications of machine learning in cyber security: A review," J. Cybersecurity Privacy, vol. 4, no. 4, pp. 972–992, Dec. 2024. DOI: 10.3390/jcp4040045. [Online]. URL: https://surl.li/vdlxkl. Accessed: 15 Jun, 2025.

[4] F. Sufi and M. Alsulami, "Mathematical modeling and clustering framework for cyber threat analysis across industries," *Mathematics*, vol. 13, no. 4, p. 655, Feb. 2025. DOI: 10.3390/math13040655. [Online]. URL: https://surl.li/fgrjnf. Accessed: 15 Jun, 2025.

[5] Y. Miao, L. Pan, et al., "Machine learning based cyber attacks targeting on controlled information: A survey," arXiv:2102.07969, Feb. 2021. [Online]. URL: https://surl.li/hmyhes. Accessed: 15 Jun, 2025.

[6] J. Vitorino, I. Praça, E. Maia, L. Sousa, and S. Jardim, "A Comparative Analysis of Machine Learning Techniques for IoT Intrusion Detection," arXiv:2111.13149, Nov. 2021. [Online]. URL: https://surli.cc/vlcuxu. Accessed: 15 Jun, 2025.

[7] H. Kavak, J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore, and S. Shetty, "Simulation for cybersecurity: State of the art and future directions," *J. Cybersecurity*, vol. 7, no. 1, p. tyab005, Mar. 2021. DOI: 10.1093/cybsec/tyab005. [Online]. URL: https://surl.lu/crguxz. Accessed: 15 Jun, 2025.

[8] XM Cyber, "Seeing what attackers see: How attack graphs help you stay ahead," Jan. 2025. [Online]. URL: https://surli.cc/dfwcym. Accessed: 15 Jun, 2025.

[9] S. Chong, J. Guttman, A. Datta, A. Myers, B. Pierce, P. Schaumont, T. Sherwood, N. Zeldovich, "Report on the NSF Workshop on Formal Methods for Security,"

Copyright © 2025, ОТА.

arXiv:1608.00678, Aug. 2016. [Online]. URL: https://surl.gd/sgrcyr. Accessed: 15 Jun, 2025.

[10] P.Y.A. Ryan, "Mathematical Models of Computer Security," in Foundations of Security Analysis and Design (FOSAD 2000), vol. 2171, Lecture Notes in Computer Science, R. Focardi and R. Gorrieri, Eds. Berlin, Germany: Springer, 2001, pp. 1–62. DOI: 10.1007/3-540-45608-2_1. [Online]. URL: https://surl.li/egqhjf. Accessed: 15 Jun, 2025.

[11] F.S. Passino, N.M. Adams, E.A.K. Cohen, M. Evangelou, and N.A. Heard, "Statistical Cybersecurity: A Brief Discussion of Challenges, Data Structures, and Future Directions," Harvard Data Science Review, vol. 5, no. 1, Mar. 2023. DOI: 10.1162/99608f92.240383c7. [Online]. URL: https://surli.cc/foscla. Accessed: 15 Jun, 2025.

[12] P. Mahadevappa, S.M. Muzammal, and R.K. Murugesan, "A Comparative Analysis of Machine Learning Algorithms for Intrusion Detection in Edge-Enabled IoT Networks," arXiv:2111.01383, Nov. 2021. [Online]. URL: https://surl.li/zwaisx. Accessed: 15 Jun, 2025.

[13] K. Mohamed, "Machine learning techniques to address cybersecurity," arXiv:2302.12415, Feb. 2023. [Online]. URL: https://surl.lu/tdmavn. Accessed: 15 Jun, 2025.

[14] D. Garton, "Purdue model framework for industrial control systems & cybersecurity segmentation," U.S. Dept. Energy/National Petroleum Council, Topic Paper 4–14, Jul. 2019. [Online]. URL: https://surli.cc/fmkjby. Accessed: 15 Jun, 2025.

[15] I. Sayar, N. Messe, S. Ebersold, and J.M. Bruel, "From What to How: A Taxonomy of Formalized Security Properties," arXiv:2505.14514, May 2025. [Online]. URL: https://surl.lu/nwovtz. Accessed: 15 Jun, 2025.

[16] Wikipedia, "Attack trees," Jan. 2025. [Online]. URL: https://surl.li/dbzvmq. Accessed: 15 Jun, 2025.

[17] Picus Security, "What is attack simulation," Jan. 2025. [Online]. URL: https://surl.li/cifqpc. Accessed: 15 Jun, 2025.

[18] Pynetlabs, "Top 10 network simulation tools," Jan. 2025. [Online]. URL: https://surl.li/qesago. Accessed: 15 Jun, 2025.

[19] Hoxhunt, "Cyber Security Simulation Training: How it Works + Best Practices," Jan. 2025. [Online]. URL: https://surl.li/cbjkeq. Accessed: 15 Jun, 2025.

[20] Picus Security, "Everything You Need to Know About BAS Tools," Jan. 2025. [Online]. URL: https://surli.cc/exllfj. Accessed: 15 Jun, 2025.

[21] Softprom, "Vulnerability management vs. penetration testing vs. breach and attack simulation," Jan. 2025. [Online]. URL: https://surl.li/afkwyc. Accessed: 15 Jun, 2025.

[22] CyberProof, "Penetration Testing vs Breach and Attack Simulator: Key Differences and Why It Matters," Jan. 2025. [Online]. URL: https://surl.li/nxbard. Accessed: 15 Jun, 2025.

[23] SCYTHE, "Top 10 breach and attack simulation (BAS) tools," Jan. 2025. [Online]. URL: https://surli.cc/ujxueh. Accessed: 15 Jun, 2025.

[24] A. Vestad and B. Yang, "A survey of agent-based modeling for cybersecurity," in *AHFE Open Access Proceedings*, vol. 127, pp. 83–93, Jul. 2024. [Online]. URL: https://surl.lu/wcoxjx. Accessed: 15 Jun, 2025.

[25] F.K. Batista, A.M. del Rey, and A. Queiruga-Dios, "A New Individual-Based Model to Simulate Malware Propagation in Wireless Sensor Networks," Mathematics, vol. 8, no. 3, p. 410, Mar. 2020. DOI: 10.3390/math8030410. [Online]. URL: https://surl.li/yvuqfp. Accessed: 15 Jun, 2025.

[26] J. Soule, J. Jamont, M. Occello, P. Theron and L. Traonouez, "Towards a multi-agent simulation of cyber-attackers and cyber-defenders battles," arXiv:2506.04849, Jun. 2025. [Online]. URL: https://surl.li/jrkiup. Accessed: 15 Jun, 2025.

[27] A. Bose, and K. Shin, "Agent-based modeling of malware dynamics in heterogeneous environments," *Security and Communication Networks*, vol. 6, no. 12, pp. 1–8, Dec. 2013. [Online]. URL: https://surl.li/akjovc. Accessed: 15 Jun, 2025.

[28] E.C. Balta, M. Pease, J. Moyne, K. Barton, and D.M. Tilbury, "Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems," IEEE Transactions on Automation Science and Engineering, vol. 21, no. 3, pp. 3245–3260, Jul. 2024. DOI: 10.1109/TASE.2023.3243147.

[29] K. Shaukat, S. Luo, V. Varadharajan, I.A. Hameed, S. Chen, D. Liu, and J. Li, "Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity," Energies, vol. 13, no. 10, p. 2509, May 2020. DOI: 10.3390/en13102509.

[30] CrowdStrike, "CrowdStrike machine learning in cybersecurity," Jan. 2025. [Online]. URL: https://surl.li/yfqmjm. Accessed: 15 Jun, 2025.

[31] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Brdalo Rapa, A.V. Grammatopoulos, and F. Di Franco, "The Role of Machine Learning in Cybersecurity," Digital Threats: Research and Practice, vol. 4, no. 1, Art. no. 8, pp. 1–38, Mar. 2023. DOI: 10.1145/3545574. [Online]. URL: https://surl.li/rpjhxe. Accessed: 15 Jun, 2025.

[32] P. Maniriho, A.N. Mahmood, and M.J.M. Chowdhury, "Deep learning models for detecting malware attacks," arXiv:2209.03622, Jan. 2024. [Online]. URL: https://surl.li/kvdwjl. Accessed: 15 Jun, 2025.

[33] M.N. Uddin, Y. Zhang, and X. Hei, "Deep learning aided software vulnerability detection: A survey," arXiv:2503.04002, Mar. 2025. [Online]. URL: https://surl.li/njcajz. Accessed: 15 Jun, 2025.

[34] M. Hesham, M. Essam, M. Bahaa, A. Mohamed, M. Gomaa, M. Hany, and W. Elsersy, "Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection," arXiv:2407.06014, Jul. 2024. [Online]. URL: https://surl.li/grzpge. Accessed: 15 Jun, 2025.

[35] B. Collins, S. Xu, and P.N. Brown, "Game-Theoretic Cybersecurity: the Good, the Bad and the Ugly,"

arXiv:2401.13815, Jan. 2024. [Online]. URL: https://surl.li/jkxpct. Accessed: 15 Jun, 2025.

[36] L. Zhang, Q. Zhu, and Y. Xie, “Improving network threat detection by knowledge graph, large language model, and imbalanced learning,” arXiv:2501.16393, May. 2025. [Online]. URL: https://surli.cc/bqlnzd. Accessed: 15 Jun, 2025.

[37] PuppyGraph, “Cyber Graph: Enhancing Cybersecurity with Graph Intelligence,” Jan. 2025. [Online]. URL: https://surl.li/yfugrw. Accessed: 15 Jun, 2025.

[38] X. Zhang, “Graph neural networks in network security: From theoretical foundations to applications,” in *Proc. Americas Conf. Inf. Syst. (AMCIS)*, Aug. 2025, pp. 1–10. [Online]. URL: https://surli.cc/wpkgob. Accessed: 15 Jun, 2025.

[39] V. Khurana and N. Kumar, “Graph Neural Networks for Cybersecurity Applications in Network Intrusion and Vulnerability Analysis,” in RADemics Research Institute, Chapter 8, Jan. 2025. [Online]. URL: https://surl.li/tchiff. Accessed: 15 Jun, 2025.

[40] Bolster.ai, “Large Language Models for Cybersecurity: The Role of LLMs in Threat Hunting,” Apr. 2025. [Online]. URL: https://surl.li/olyczz. Accessed: 15 Jun, 2025.

[41] H. Xu, and et al., “Large language models for cyber security: A systematic literature review,” arXiv:2405.04760, Jul 2024. [Online]. URL: https://surl.li/coqqui. Accessed: 15 Jun, 2025.

[42] Z. Liu, “Multi-Agent Collaboration in Incident Response with Large Language Models,” arXiv:2412.00652, Dec. 2024. [Online]. URL: https://surl.li/aghvvq. Accessed: 15 Jun, 2025.

[43] E. Mezzi, F. Massacci, and K. Tuma, “Large language models are unreliable for cyber threat intelligence,” arXiv:2503.23175, Mar. 2025. [Online]. URL: https://surl.lu/xonjqn. Accessed: 15 Jun, 2025.

[44] V. Kravchuk, N. Maslova, and I. Dorohyi, “Automated xss vulnerability detection in web applications based on a multi-agent approach”, SP DonNTU. OTA, vol. 3, no. 4 (36), pp. 13–26, May 2025.

Стаття надійшла до редакції 20.09.2025
Стаття прийнята 05.10.2025
Статтю опубліковано

Copyright © 2025, OTA.